BURMISTRZ
MIASTA LUBAWKA
woj. dolnośląskie

ZARZĄDZENIE NR 16/2016

BURMISTRZA MIASTA LUBAWKA

z dnia 01.03.2016 r.

w sprawie: **wprowadzenia polityki bezpieczeństwa Informacji w Urzędzie Miasta Lubawka oraz przyjęcia instrukcji zarządzania systemem informatycznym.**

Na podstawie: art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j.t. Dz.U. z 2015 poz. 2135 ze zm.) oraz § 3 ust. 3, § 4, § 5 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100 poz. 1024) oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 o samorządzie gminnym (j.t. Dz.U. z 2015 r. poz. 1515 ze zm.) zarządza się, co następuje:

§1

1. Wprowadza się „Politykę Bezpieczeństwa Informacji w Urzędzie Miasta Lubawka" zwana dalej „Polityką", która stanowi załącznik 1 do niniejszego zarządzenia.
2. Wprowadza się „Instrukcję Zarządzania Systemem Informatycznym", zwaną dalej „Instrukcją", która stanowi załącznik 2 do niniejszej umowy.

§2

Zobowiązuje się pracowników Urzędu Miasta Lubawka do stosowania zasad określonych w „Polityce" i „Instrukcji".

§3

Zarządzenie wchodzi w życie z dniem podpisania.

RADCA PRAWNY
Piotr Krystowski

BURMISTRZ
Ewa Kocemba

Załącznik Nr1
do Zarządzenia Nr 16/2016
Burmistrza Miasta Lubawka
z dnia 01 marca 2016

POLITYKA BEZPIECZEŃSTWA INFORMACJI

W URZĘDZIE MIASTA LUBAWKA

Rozdział I

Postanowienia ogólne, definicje i objaśnienia

§1.
Zawartość opracowania, definicje i objaśnienia

1. Polityka Bezpieczeństwa Informacji Urzędu Miasta Lubawka jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych we wszystkich zbiorach danych osobowych administracyjnych przez Urząd Miasta Lubawka.

2. Podstawą do opracowania i wdrożenia dokumentu są:

   - Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997r. (Dz. U. z 1997r., 78 poz. 483 ze zm.)

   - ustawa z dnia 29.08.1997 o ochronie danych osobowych (Dz. U. z 2015r. poz. 2135 ze zm.)

   - rozporządzenie MSWiA z dnia 27.04.2004 w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r., nr 100 poz. 1024 ze zm.)

3. Polityka Bezpieczeństwa Informacji Urzędu Miasta Lubawka zawiera m.in.
   - wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe, stanowiący załącznik numer 1 do niniejszej polityki bezpieczeństwa informacji
   - wykaz zbiorów danych osobowych przetwarzanych elektronicznie lub w inny sposób, stanowiący załącznik numer 2 do niniejszej polityki bezpieczeństwa informacji
   - opis struktury zbiorów danych przetwarzanych w systemach informatycznych oraz sposób przepływu danych pomiędzy systemami informatycznymi, stanowiący załącznik numer 3 do polityki bezpieczeństwa informacji.
   - sposób przepływu danych pomiędzy poszczególnymi systemami (załącznik nr 3 do „Polityki Bezpieczeństwa Informacji");
   - określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych (Załącznik nr 2do Zarządzenia nr 16/2016, rozdział nr 3).

§2.
Definicje stosowane w polityce bezpieczeństwa informacji

Użyte w treści polityki bezpieczeństwa informacji określenia oznaczają:

1. **Ustawa** - ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2015 poz. 2135 ze zm.)
2. **Urząd** - Urząd Miasta Lubawka
3. **Administrator Danych Osobowych** – Burmistrz Miasta Lubawka zwany dalej **ADO**
4. **Administrator Bezpieczeństwa Informacji** – pracownik urzędu lub inna osoba wyznaczona przez ADO, do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie, oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych, zwana dalej **ABI**, powołany Zarządzeniem Burmistrza
5. **Administrator Systemów Informatycznych**, zwany dalej **ASI** - osoba odpowiedzialna za przestrzeganie zasad ochrony danych osobowych i nadzorująca bezpieczeństwo przetwarzania danych osobowych, powołany Zarządzeniem Burmistrza.
6. **System informatyczny** – zespół środków technicznych (urządzenia komputerowe, drukujące, łączności w raz z okablowaniem i oprogramowaniem), zespół zabezpieczeń środków technicznych, użytkownicy tych urządzeń i programów, a także sieć informatyczna i udostępniane przez nią zasoby.
7. **Dane osobowe** – zestaw informacji pozwalających na jednoznaczną identyfikację konkretnej osoby w konkretnym środowisku pracy
8. **Zbiór danych** – każdy posiadający strukturę zbiór danych o charakterze osobowym, dostępnym wg określonych kryteriów
9. **Przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbierania, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie niezależnie od formy, w jakiej wykonywane są te czynności.
10. **Osoby przetwarzające dane osobowe** – wszystkie osoby, w tym użytkownicy systemu informatycznego, mające- z racji wykonywanych obowiązków na podstawie umowy o pracę, zlecenie, odbywanie praktyki, stażu – dostęp do danych osobowych

11. **Lokalny administrator bezpieczeństwa informacji** – kierownik, osoba odpowiedzialna za przestrzeganie zasad przetwarzania i ochrony danych w podległej sobie komórce organizacyjnej

§3.

Zadania administratora danych osobowych

1. Administrator danych osobowych ma obowiązek stosować środki techniczne i organizacyjne zapewniających ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczać dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Administrator danych osobowych określa zakres przetwarzanych danych osobowych w wydawanych zarządzeniach, regulaminach lub w indywidualnych umowach podmiotami zewnętrznymi, którym zlecono przetwarzanie danych osobowych.
3. Administrator danych osobowych przetwarza dane osobowe znajdujące się w administrowanych przez niego zbiorach w określonych celach i w określonym zakresie, jeżeli:

   - jest to konieczne do określonych prawem zadań,

   - jest to niezbędne do osiągnięcia uzasadnionych celów,

   - w innym celu i zakresie, jeśli osoba, której przetwarzane dane dotyczą, wyrazi na to pisemną zgodę,

4. W przypadkach szczególnych cel i zakres przetwarzanych danych mogą określać inne obowiązujące przepisy szczegółowe.

§4.

Obowiązki związane z dostępem do danych osobowych

1. Dostęp do zbioru danych osobowych oraz ich przetwarzania mają tylko osoby wpisane do ewidencji prowadzonej przez administratora bezpieczeństwa informacji – załącznik Nr 4 do niniejszej polityki bezpieczeństwa.

2. Osoby zatrudnione w Urzędzie Miasta Lubawka przy przetwarzaniu danych osobowych są zobowiązane do przechowywania danych osobowych we właściwych zbiorach, nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania.

3. Osoby zatrudnione w Urzędzie Miasta Lubawka przy przetwarzaniu danych osobowych przy wykorzystaniu systemów informatycznych są zobowiązane do postępowania zgodnie z „Instrukcją zarządzania systemem informatycznym" służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji".

§5

1. Osoby zatrudnione przy przetwarzaniu danych są zobowiązane powiadomić administratora bezpieczeństwa informacji o ewentualnych naruszeniach bezpieczeństwa systemu ochrony danych osobowych w każdym zbiorze danych lub systemie.

2. W skład systemu wchodzą:

   - dokumentacja papierowa (korespondencja obywateli, firm, innych instytucji publicznych i niepublicznych, formularze zgody na przetwarzanie danych osobowych, itd.),

   - urządzenia i oprogramowanie komputerowe służące do przetwarzania informacji oraz procedury przetwarzania danych w tym systemie, w tym procedury awaryjne,

   - wydruki komputerowe.

3. W przypadku stwierdzenia naruszenia ochrony danych osobowych należy bezzwłocznie:

   - powiadomić Administratora Bezpieczeństwa Informacji lub bezpośredniego przełożonego,

   - zablokować dostęp do systemu dla użytkowników praz osób nieupoważnionych,

   - niezwłocznie podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony (o ile to możliwe),

   - zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia bezpieczeństwa systemu,

   - zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia.

4. Po przybyciu na miejsce naruszenia bezpieczeństwa danych osobowych, Administrator Bezpieczeństwa informacji lub osoba przez niego upoważniona, podejmuje czynności wyjaśniające mające na celu ustalenie:

   - przyczyn i okoliczności naruszenia ochrony,

   - zapoznania się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości pracy urzędu,

   - osób winnych naruszenia danych osobowych,

   - skutków naruszenia, w tym rozważa celowość kontaktu ze specjalistami spoza urzędu (jeśli zachodzi taka potrzeba).

5. Administrator Bezpieczeństwa Informacji zobowiązany jest do powiadomienia Burmistrza Miasta Lubawka, który podejmuje czynności zmierzające do przywrócenia poprawnej pracy systemu oraz o ponownym przystąpieniu do pracy w systemie.

6. Administrator Bezpieczeństwa Informacji zobowiązany jest do sporządzenia pisemnego raportu na temat zaistniałej sytuacji zawierającego co najmniej (załącznik nr 5):

   - datę i miejsce zawiadomienia o naruszeniu bezpieczeństwa, jak i samego naruszenia (o ile da się ustalić),

   - wskazanie osoby zawiadamiającej o naruszeniu oraz innych osób zaangażowanych w wyjaśnienie okoliczności naruszenia bezpieczeństwa,

   - określenie okoliczności towarzyszących i rodzaju naruszenia,

   - opis podjętego działania wraz z wyjaśnieniem wyboru sposobu działania, wstępną ocenę przyczyn wystąpienia naruszenia bezpieczeństwa,

   - ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

7. Raport z wystąpienia zdarzenia ABI przekazuje ADO.

8. ABI zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych). Zaistniałe naruszenie bezpieczeństwa może stać się przedmiotem zespołowej analizy przeprowadzanej przez kierownictwo urzędu, ADO, ABI i Pełnomocnika ds. Informacji Niejawnych. Analiza ta powinna zawierać wszechstronną ocenę zaistniałego naruszenia bezpieczeństwa, wskazanie odpowiedzialnych, wnioski co do ewentualnych działań proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.

§ 6

Zakazy przetwarzania danych wrażliwych

W zbiorach danych administrowanych przez Urząd zabrania się przetwarzania danych ujawniających:

1. stan zdrowia,
2. pochodzenie rasowe lub etniczne,
3. poglądy polityczne,
4. przekonania religijne lub filozoficzne,
5. przynależność wyznaniową,
6. przynależność partyjną lub związkową,
7. kod genetyczny,
8. nałogi,
9. preferencje seksualne,

chyba że wymagają tego obowiązujące przepisy prawa lub osoba, której powyższe dane dotyczą wyraziła pisemną zgodę.

§ 7

Odpowiedzialność służbowa

Pracownik, który:

1. przetwarza w zbiorze danych dane osobowe
   - do których przetwarzania nie jest upoważniony,
   - których przetwarzanie jest zabronione,
   - niezgodne z celem stworzenia zbioru danych;
2. udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym,
3. nie zgłasza ABI zbiorów danych podlegających rejestracji,
4. nie dopełnia obowiązku poinformowania osoby, której dane dotyczą przysługujących jej prawach,
5. uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw,

podlega odpowiedzialności karnej zgodnie z ustawą oraz sankcjami określonymi w Kodeksie pracy.

Rozdział II

Gromadzenie danych osobowych

§ 8

Gromadzenie danych osobowych

Dane osobowe przetwarzane w Urzędzie mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą lub z innych źródeł, w granicach dozwolonych przepisami prawa.

§ 9

Wykorzystywanie danych osobowych

1. Zebrane dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu, dane powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.
2. W przypadku konieczności udostępnienia dokumentów i danych, wśród Których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

Rozdział III

Udzielanie informacji o przetwarzaniu danych osobowych

§ 10

Kontrola własnych danych osobowych

1. Osobom, których dane osobowe przetwarza się w zbiorze danych Urzędu przysługuje, zgodnie z ustawą, prawo kontroli ich danych osobowych, a w szczególności prawo do uzyskania wyczerpujących informacji na temat tych danych.
2. Każda osoba, która wystąpi z wnioskiem o otrzymanie informacji, powinna otrzymać odpowiedź w formie pisemnej, w terminie nie dłuższym niż 30 dni od daty wpływu wniosku do Urzędu.

§ 11

Obowiązek uzupełniania danych

W przypadku, gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały

zebrane, ABI jest zobowiązany do ich uzupełnienia, zaktualizowania, sprostowania lub usunięcia.

Rozdział IV

Rejestracja zbiorów danych osobowych

§ 12

Obowiązki kierowników komórek organizacyjnych

Kierownicy komórek organizacyjnych Urzędu, w których przetwarzane są dane osobowe, są zobowiązani do zgłoszenia ABI informacji na temat:

1. Planowanego założenia nowych zbiorów danych osobowych wymagających rejestracji,
2. Wnoszonych zmian do zbiorów już zarejestrowanych.

Rozdział V

Ochrona przetwarzania danych osobowych

§ 13

Przechowywanie imiennych upoważnień do przetwarzania danych osobowych

1. ADO Urzędu zobowiązany jest do wydawania, ewidencjonowania i przechowywania imiennych upoważnień do przetwarzania danych osobowych oraz cofniętych upoważnień. Upoważnienie może zostać wydane na czas określony lub do odwołania. Wzory formularza upoważnienia i formularza cofnięcia upoważnienia stanowią załącznik nr 6 do niniejszej polityki bezpieczeństwa informacji.
2. Osoby przetwarzające dane osobowe są zobowiązane zapoznać się z ustawą o ochronie danych osobowych, niniejszą polityka bezpieczeństwa i instrukcją zarządzania systemem informatycznym i stosować ich przepisy na swoim stanowisku pracy.
3. ADO Urzędu zobowiązany jest do zbierania, ewidencjonowania i przechowywania oświadczeń osób przetwarzających dane osobowe o zachowaniu tajemnicy danych, z którymi mają styczność i znajomości przepisów. Wzór formularza oświadczenia stanowi załącznik nr 7 do niniejszej polityki bezpieczeństwa informacji.
4. Oświadczenie przechowuje się w aktach osobowych pracownika.

5. Brak ważnego upoważnienia, o którym mowa w pkt. 1 oraz brak podpisanego oświadczenia, którym mowa w pkt. 3, uniemożliwia powierzenie pracownikowi wykonywania zadań związanych z przetwarzaniem danych osobowych.

§14

Obowiązki Administratora Bezpieczeństwa Informacji – ABI

1. Całkowity nadzór i kontrola przetwarzania danych osobowych w Urzędzie realizuje i odpowiada za te działania ABI.
2. ABI ma obowiązek ściśle współpracować z administratorem systemu informatycznego – ASI w zakresie przetwarzania danych osobowych w systemach informatycznych.
3. ABI ma obowiązek zapewnić zapoznanie się osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami dotyczącymi ochrony danych osobowych oraz przeszkolić je w tym zakresie.

§ 15

Prawa ABI

W celu realizacji powierzonych zadań ABI w Urzędzie ma prawo:

1. kontrolować komórki organizacyjne Urzędu w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe,
2. wydawać polecenia kierownikom komórek organizacyjnych Urzędu Miasta Lubawka w zakresie bezpieczeństwa danych osobowych,
3. informować ADO Urzędu o przypadkach naruszenia bezpieczeństwa danych osobowych,
4. żądać od wszystkich pracowników Urzędu wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.

Rozdział VI

Zasady udostępniania danych osobowych

§ 16

Osoby uprawnione do wglądu do danych osobowych

ADO udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.

§ 17

Tryb udostępniania danych osobowych

1. Zbiory danych osobowych udostępnia się na pisemny, umotywowany wniosek chyba, że odrębne przepisy prawa stanowią inaczej.
2. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie.
3. Wniosek o udostępnienie danych osobowych jest rozpatrywany przez lokalnego administratora bezpieczeństwa informacji lub w przypadku jego nieobecności – ABI.
4. Decyzję w sprawie udostępnienia danych podejmuje lokalny administrator bezpieczeństwa informacji lub przypadku jego nieobecności – ABI.

§ 18

Odmowa udostępnienia informacji

ADO może odmówić udostępnienia danych osobowych, jeżeli spowodowałoby to istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

§ 19

Powierzenie przetwarzania danych osobowych

1. ADO może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej.
2. Podmiot, o którym mowa w ust. 1, jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych.
3. Podmiot, o którym mowa w ust. 1, jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie określonym w umowie.
4. W przypadkach opisanych w ust, 1-3 odpowiedzialność za ochronę danych osobowych spoczywa na ADO, co nie wyklucza odpowiedzialności podmiotu, z którym zawarto umowę z tytułu przetwarzania danych osobowych niezgodnie z umową.
5. Przy kontroli zgodności przetwarzanych danych przez upoważniony przez ADO podmiot, o którym mowa w ust. 1, stosuje się odpowiednio przepisy art. 14-19 ustawy.

Rozdział VII

Postanowienia końcowe

§ 20

Odpowiedzialność

1. Zobowiązuje się użytkowników systemu do zachowania tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczeń, zgodnie z art. 39 ust. 2 ustawy również po ustaniu stosunku pracy oraz do przestrzegania instrukcji i procedur związanych z ochroną danych osobowych.
2. Wobec osoby, która w przypadku naruszenia ochrony danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby, zgodnie z określonymi zasadami, wszczyna się postępowanie dyscyplinarne.
3. Kara dyscyplinarna wobec osoby uchylającej się od powiadomienia ABI nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą o ochronie danych osobowych.

Załącznik Nr 1

do „Polityki Bezpieczeństwa Informacji

w Urzędzie Miasta Lubawka"

WYKAZ BUDYNKÓW I POMIESZCZEŃ, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

1. Urząd Miasta Lubawka – 58-420 Lubawka, ul. Plac Wolności 1

Załącznik Nr 2

do „Polityki Bezpieczeństwa Informacji

w Urzędzie Miasta Lubawka"

WYKAZ ZBIORÓW DANYCH OSOBOWYCH PRZETWARZANYCH ELEKTRONICZNIE LUB W INNY SPOSÓB W URZEDZIE MIASTA LUBAWKA

1. Zbiór dotyczący zwrotu opłaty skarbowej, zawiera: imię i nazwisko, adres, numer konta.
2. Ewidencja gruntów i budynków, zawiera: imię i nazwisko, adres, nr działki, nr mapy, nr księgi wieczystej, PESEL, imię ojca, imię matki.
3. Elektroniczny obieg dokumentów, zawiera: imię i nazwisko, adres, nr telefonu.
4. Zbiór dokumentów dotyczących rozgraniczenia i podziałów nieruchomości, zawiera: imię i nazwisko, adres, nr działki, nr mapy, nr księgi wieczystej.
5. Zbiór dokumentów związanych z przejęciem nieruchomości, zawiera: imię i nazwisko, adres, nr działki, nr mapy, nr księgi wieczystej, nr konta.
6. Zbiór dokumentów o ustaleniu opłaty adiacenckiej, zawiera: imię i nazwisko, adres, nr działki, nr mapy, nr księgi wieczystej.
7. Zbiór dokumentów dotyczący wycinki drzew i krzewów, zawiera: imię i nazwisko, adres, nr działki, nr mapy, nr księgi wieczystej.
8. Zbiór dokumentów dotyczących dobierania zwierząt właścicielowi, zawiera: imię i nazwisko, adres.
9. Zbiór dokumentów w sprawie nakazu uprzątnięcia odpadów z miejsc nie przeznaczonych do ich składowania, zawiera: imię i nazwisko, adres, nr działki, karta mapy.
10. Zbiór dotyczący wymierzania administracyjnej kary pieniężnej za usuwanie drzew i krzewów bez zezwolenia, zawiera: imię i nazwisko, adres, nr działki, karta mapy.
11. Zbiór dokumentów dotyczących adopcji bezpańskich zwierząt, zawiera: imię i nazwisko, adres.
12. Zbiór dokumentów dotyczących obowiązkowego ubezpieczenia OC gospodarstwa rolnego, zawiera: imię i nazwisko, adres.
13. Zbiór dokumentów dotyczących wyceny wartości drewna, oszacowania gatunków drzew, zawiera: imię i nazwisko, adres, PESEL, nr działki, karta mapy.

14. Zbiór dotyczący prowadzenia gospodarstwa rolnego, zawiera: imię i nazwisko, adres.

15. Zbiór dokumentów dotyczący zbiorników bezodpływowych i przydomowych oczyszczalni ścieków, zawiera: imię i nazwisko, adres, nr działki, karta mapy.

16. Zbiór dokumentów dotyczących środowiskowych postępowań, zawiera: imię i nazwisko, adres, nr działki, karta mapy.

17. Zbiór dokumentów dotyczących oddania gruntów mienia gminnego w użytkowanie wieczyste, zawiera: imię i nazwisko, adres.

18. Zbiór dotyczący dzierżawy mienia gminnego, zawiera: imię i nazwisko, adres, nr konta.

19. Zbiór dotyczący przekształcenia prawa użytkowania wieczystego w prawo własności, zawiera: imię i nazwisko, adres, nr konta.

20. Zbiór dokumentów dotyczących posiadania psów ras uznawanych za agresywne, zawiera: imię i nazwisko, adres.

21. Zbiór dokumentów dotyczących sprzedaży mienia gminnego, zawiera: imię i nazwisko, adres.

22. Zbiór dokumentów dotyczących wyrobów zawierających azbest, zawiera: imię i nazwisko, adres, nr działki, karta mapy, księga wieczysta, NIP, PESEL, nr konta.

23. Zbiór dokumentów dotyczących gospodarki odpadami, zawiera: imię i nazwisko, PESEL, adres, nr telefonu, adres email, miejsce pracy, stan zdrowia.

24. Zbiór dokumentów dotyczących planów urządzenia lasów niepaństwowych, zawiera: imię i nazwisko, adres, nr działki, karta mapy.

25. Zbiór aktów notarialnych, zawiera: imię i nazwisko, adres, nr działki, nr mapy, nr księgi wieczystej.

26. Zbiór postanowień o nabyciu spadku, zawiera: imię i nazwisko, adres, nr działki, nr księgi wieczystej.

27. Zbiór postanowień o zasiedzeniu nieruchomości, zawiera: imię i nazwisko, adres, nr działki, nr księgi wieczystej.

28. Zbiór dokumentów dotyczących planu zagospodarowania przestrzennego, zawiera: imię i nazwisko, adres, nr działki, nr mapy.

29. Zbiór dokumentów dotyczących opłaty planistycznej, zawiera: imię i nazwisko, adres, nr działki, nr mapy, nr księgi wieczystej.

30. Zbiór dokumentów dotyczących nadania numeru porządkowego nieruchomości, zawiera: imię i nazwisko, adres, nr działki, nr mapy, rodzaj budynku przed i po zmianie.

31. Zbiór decyzji na budowę, rozbudowę, zmianę sposobu użytkowania budynku, zawiera: imię i nazwisko, adres, nr działki, nr mapy.
32. Zbiór zawiadomień o zakończeniu budowy, zawiera: imię i nazwisko, adres, nr działki.
33. Zbiór dokumentów dotyczących wynajmu lokali komunalnych, zawiera: imię i nazwisko, adres.
34. Zbiór dokumentów dotyczących odprowadzania ścieków i dostarczania wody, zawiera: imię i nazwisko, adres.
35. Wykaz osób podlegających obowiązkowi i szkoleniom w zakresie powszechnej samoobrony, zawiera: imię i nazwisko, adres, rok urodzenia.
36. Ewidencja osób wyznaczonych do pełnienia służby w formacjach obrony cywilnej, zawiera: Imię i nazwisko, imię ojca, stopień wojskowy, data urodzenia, adres zamieszkania, stanowisko w FOC, nr karty przydziału.
37. Zbiór dotyczący ekwiwalentu i badań lekarskich członków OSP, zawiera: imię i nazwisko, adres, nr konta, PESEL, orzeczenie lekarskie.
38. Akta urzędu stanu cywilnego, zawierają: nazwisko i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, PESEL, miejsce pracy, zawód, nazwisko rodowe, nazwisko z poprzedniego małżeństwa, miejsce i godzina urodzenia, data i numer aktu zgonu, data i numer aktu małżeństwa, data i numer aktu urodzenia, imię i nazwisko ojca, imię i nazwisko matki, imię i nazwisko współmałżonka, płeć, stan cywilny, data i miejsce zawarcia małżeństwa, miejsce wystawienia i numer aktu urodzenia żony/męża, data, godzina i miejsce zgonu, odnalezienia zwłok, data zgonu żony/męża, imię, nazwisko i adres osoby zgłaszającej zgon, numer aktu zgonu żony/męża, imię i nazwisko rodowe małżonka, nazwisko rodowe ojca, nazwisko rodowe matki, dane dotyczące rozwodu, nazwisko po zawarciu małżeństwa, numer dowodu osobistego i miejsce jego wydania, PESEL, dane dotyczące uznania/zaprzeczenia ojcostwa i przysposobienia – data i numer orzeczenia sądu, imię i nazwisko przysposabiającego, zmiana nazwiska dziecka, data rozwiązania poprzedniego małżeństwa.
39. Ewidencja ludności, zawiera: nazwisko i imiona, nazwisko rodowe, imiona rodziców, nazwiska rodowe rodziców, data urodzenia, miejsce urodzenia, numery aktów urodzenia, małżeństwa i zgonu, adres zameldowania, PESEL, seria i numer dokumentu tożsamości, płeć, kod pocztowy, kod terytorialny, stan cywilny, imię i nazwisko rodowe współmałżonka, obywatelstwo, dane o zgonie, imię i nazwisko oraz seria i numer dowodu osobistego właściciela nieruchomości.
40. Zbiór dowodów osobistych, zawiera: nazwisko i imiona, nazwisko rodowe, imiona rodziców, nazwisko rodowe matki, data urodzenia, miejsce urodzenia, adres

zameldowania, PESEL, seria i numer dowodu osobistego, płeć, wzrost w cm, kolor oczu, wizerunek twarzy, kod pocztowy, kod terytorialny.

41. Zbiór osób z dostępem do informacji niejawnych, zawiera: imiona i nazwisko, nazwisko rodowe, data i miejsce urodzenia, PESEL, NIP, adres zamieszkania i zameldowania, nr i seria dowodu osobistego, paszportu oraz wojskowego dokumentu tożsamości, miejsce zatrudnienia lub prowadzenia firmy warz z adresem i zajmowanym stanowiskiem, informacja o karalności, informacja o indagowaniu przez obce władze lub służby, kontakty prywatne i służbowe z obywatelami innych państw, stan zdrowia, sytuacja majątkowa.

42. Kwalifikacja wojskowa, zawiera: imię i nazwisko, nazwisko rodowe, data i miejsce urodzenia, PESEL, adres i data zameldowania na pobyt stały, stopień wojskowy, nazwa, seria i numer wojskowego dokumentu tożsamości, seria i numer dowodu osobistego, kategoria zdrowia.

43. Rejestr osób objętych kwalifikacją wojskową, zawiera: imię i nazwisko, nazwisko rodowe, imiona i nazwiska rodowe rodziców, datę i miejsce urodzenia, PESEL, adres i data zameldowania na pobyt stały i czasowy.

44. Rejestr wyborców, zawiera: nazwisko i imiona, PESEL, imię ojca, adres zameldowania, adres, pod którym wyborca wpisany jest do stałego rejestru wyborców.

45. Wykaz osób stanowiących obsadę gminnego stanowiska kierowania, zawiera: imię i nazwisko, adres zamieszkania, numery telefonów.

46. Wykaz osób stanowiący obsadę stałego dyżuru, zawiera: imię i nazwisko, adres zamieszkania, numery telefonów.

47. Zbiór decyzji nakładających obowiązek świadczeń osobistych lub rzeczowych, zawiera: imię i nazwisko, adres zamieszkania.

48. Zbiór dokumentów dotyczących podatku od środków transportowych, zawiera: imię i nazwisko, data urodzenia, adres zamieszkania.

49. Zbiór dokumentów dotyczących podatku od nieruchomości, zawiera: imię i nazwisko, PESEL, imiona rodziców, data urodzenia, adres, powierzchnie i klasy działek.

50. Zbiór dokumentów dotyczących akcyzy, zawiera: imię i nazwisko, PESEL. NIP, adres, imiona rodziców, data urodzenia, nr konta bankowego, powierzchnie klasy gruntów.

51. Zbiór dokumentów dotyczących podatku rolnego, zawiera: imię i nazwisko, data urodzenia, PESEL, imiona rodziców, adres, nr działek, nr telefonu, powierzchnie i klasy gruntów.

52. Zbiór dokumentów dotyczących podatku leśnego, zawiera: imię i nazwisko, data urodzenia, PESEL, imiona rodziców, adres, nr działek, nr telefonu.

53. EDG i CEIDG, zawiera: imię i nazwisko, nazwisko rodowe, imiona rodziców, data i miejsce urodzenia, adres zamieszkania, zameldowania, adres do korespondencji, adres email, miejsce działalności, PESEL, NIP, REGON, obywatelstwo, płeć.

54. Zbiór dokumentów dotyczących sprzedaży napojów alkoholowych, zawiera: imię i nazwisko, adres.

55. Zbiór dokumentów w sprawie zajęcia pasa drogowego, zawiera: imię i nazwisko, adres, nr działki, nr telefonu.

56. Zbiór dokumentów dotyczących dofinansowania kosztów kształcenia młodocianego pracownika, zawiera: imię nazwisko pracownika, datę urodzenia, adres, zaświadczenie o zdaniu egzaminu w zawodzie.

57. Zbiór testamentów, zawiera: imię i nazwisko, datę urodzenia, imiona rodziców, adres.

58. Zbiór dokumentów dotyczących pracowników Urzędu Miasta Lubawka, zawiera: imię i nazwisko, data i miejsce urodzenia, imiona rodziców, nazwisko rodowe matki, PESEL, NIP, stopień wojskowy i nr książeczki wojskowej, miejsce zamieszkania i zameldowania, adres do korespondencji, nr telefonu, wykształcenie i dodatkowe uprawnienia, seria i nr dowodu osobistego, dane dotyczące niepełnosprawności, zajmowane stanowisko, orzeczenie lekarskie o dopuszczeniu (lub nie) do pracy na danym stanowisku, nr konta bankowego.

59. Zbiór dokumentów dotyczących osób startujących w naborze na stanowiska, zawiera: imię i nazwisko, data i miejsce urodzenia, imiona rodziców, PESEL, miejsce zamieszkania lub zameldowania, adres do korespondencji, nr telefonu, wykształcenie i dodatkowe uprawnienia, seria i nr dowodu osobistego, dane dotyczące niepełnosprawności.

60. Zbiór dokumentów dotyczących osób odbywających karę ograniczenia wolności lub prace społecznie użyteczne, zawiera: imię i nazwisko, data urodzenia, adres.

61. Zbiór umów dzierżawy pomiędzy osobami fizycznymi, zawiera: imię nazwisko, adres, nr działek.

62. Oświadczenia majątkowe, zawierają: imię i nazwisko, data urodzenia, adres zamieszkania, PESEL, miejsce pracy, wysokość dochodów.

63. Zbiór radnych Gminy Lubawka, zawiera: imię i nazwisko, adres, data urodzenia, NIP, PESEL, nr telefonu, adres email, wykształcenie, nr konta bankowego.

64. Zbiór sołtysów Gminy Lubawka, zawiera: imię i nazwisko, adres, nr telefonu, nr konta bankowego.

65. Dziennik korespondencyjny (poczta przychodząca i wychodząca), zawiera: imię i nazwisko, adres.

66. Zbiór wniosków i decyzji w sprawie pomocy materialnej dla uczniów o charakterze socjalnym, stypendia szkolne, stypendia sportowe, zawiera: imię i nazwisko, adres, data urodzenia, PESEL, wysokość dochodów.

Załącznik Nr 3

do „Polityki Bezpieczeństwa Informacji

w Urzędzie Miasta Lubawka"

OPIS STRUKTURY ZBIORÓW DANYCH OSOBOWYCH PRZETWARZANYCH W SYSTEMACH INFORMATYCZNYCH ORAZ SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY SYSTEMAMI INFORMATYCZNYMI

Do przetwarzania danych osobowych w systemie informatycznym urzędu stosuje się aplikacje:

- Prokom Płatnik,
- Pomoc materialna dla uczniów,
- Ewidencja działalności gospodarczej,
- Koncesje alkoholowe,
- Baza opłat za użytkowanie wieczyste,
- Bazy reset i raf soft – rachunki,
- Baza systemu finasowo-księgowego,
- Baza podatków od środków transportu,
- Baza podatków od gruntów i nieruchomości,
- Baza dodatków mieszkaniowych,
- Baza obiegu dokumentów,
- Baza windykacji opłat i podatków,
- Baza kadry – płace,
- Baza środków trwałych,
- Powszechny Elektroniczny System Ewidencji Ludności,
- Lokalna baza ewidencji ludności,
- Rejestr Dowodów Osobistych,
- Baza Usług Stanu Cywilnego.

Skąd	Dokąd	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych
Kadry	Płatnik ZUS	=>	eksport/import pliku
Płace	Płatnik ZUS	=>	eksport/import pliku
Płace	System bankowy	=>	eksport/import pliku
e-Pfron	Pfron	=>	transmisja bezpośrednio z programu
Płatnik	ZUS	=>	transmisja bezpośrednio z programu
Baza Usług Stanu Cywilnego	Powszechny Elektroniczny System Ewidencji Ludności	=>	transmisja bezpośrednio z programu
Powszechny Elektroniczny System Ewidencji Ludności	Lokalna baza ewidencji ludności	=>	transmisja bezpośrednio z programu
Baza Usług Stanu Cywilnego	Rejestr Dowodów Osobistych	=>	transmisja bezpośrednio z programu
Powszechny Elektroniczny System Ewidencji Ludności	Rejestr Dowodów Osobistych	=>	transmisja bezpośrednio z programu
Baza Usług Stanu Cywilnego	Główny Urząd Statystyczny	=>	transmisja bezpośrednio z programu
Platforma operacyjna ZK	Urząd Wojewódzki Zarządzanie Kryzysowe	=>	transmisja bezpośrednio z programu

Pozostałe programy działają niezależnie w oparciu o własne bazy danych i nie posiadają wbudowanego mechanizmu umożliwiającego przepływ danych osobowych pomiędzy innymi systemami informatycznymi stosowanymi w Urzędzie Miasta Lubawka.

Załącznik Nr 4

do „Polityki Bezpieczeństwa Informacji

w Urzędzie Miasta Lubawka"

Wykaz osób, które zostały zapoznane z „Polityką ochrony danych osobowych w Urzędzie Miasta Lubawka" oraz „Instrukcją Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Lubawka"

L.p.	Imię i nazwisko	Stanowisko	Data	Podpis

Załącznik Nr 5

do „Polityki Bezpieczeństwa Informacji

w Urzędzie Miasta Lubawka"

Raport z naruszenia bezpieczeństwa danych osobowych w Urzędzie Miasta Lubawka

1. Data ..... Godzina .....
2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....

(imię, nazwisko, stanowisko służbowe, nazwa użytkownika – jeżeli występuje)

3. Lokalizacja zdarzenia

.....

(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

Przyczyny wystąpienia zdarzenia:

.....

.....

5. Podjęte działania:

.....

.....

6. Postępowanie wyjaśniające:

.....

.....

.....

.....

(data, podpis Administratora Bezpieczeństwa Informacji)

Załącznik Nr 6

do „Polityki Bezpieczeństwa Informacji

w Urzędzie Miasta Lubawka"

Lubawka, dnia .....

UPOWAŻNIENIE IMIENNE NR .....

DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy a dnia 29 sierpnia 1997r. o ochronie danych osobowych (t.j. Dz. U. z 2014r. poz. 1182 ze zm.), upoważniam / cofam upoważnienie dla Pani / Pana:

.....

(imię i nazwisko osoby upoważnionej)

zatrudnioną / zatrudnionego w:

.....

(nazwa komórki organizacyjnej)

na stanowisku: .....

do przetwarzania danych osobowych w zakresie .....

.....

.....

Upoważnienie ważne na czas .....

.....

(podpis Administratora Danych Osobowych)

Załącznik Nr 7

do „Polityki Bezpieczeństwa Informacji

w Urzędzie Miasta Lubawka"

.....

Nazwisko i imię

.....

Stanowisko/zlecenie/praktyka/staż

Oświadczenie

Oświadczam, że w związku z wykonywaniem obowiązków, przetwarzam oraz mam dostęp do zbiorów, dokumentów, zestawień, kartotek lub systemów informatycznych zawierających dane osobowe i w związku z tym zapoznałem(am) się z:

1. ustawą z dnia 29.08.1997r. o ochronie danych osobowych (Dz. U. z 2015r. poz. 2135 ze zm.),
2. rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. nr 100, poz. 1024 ze zm.),
3. polityką bezpieczeństwa informacji,
4. instrukcją zarządzania systemem informatycznym.

Zobowiązuję się w okresie odbywania pracy/stażu/praktyki/umowy zlecenia, jak również po ustaniu, do zachowania tajemnicy wszystkich danych osobowych, do których będę miał(a) dostęp w związku z wykonywaniem obowiązków.

Jestem świadomy(a) odpowiedzialności karnej za udostępnienie lub umożliwienie dostępu do danych osobowych osobom nieupoważnionym.

.....

(podpis pracownika)

Załącznik Nr 2

do Zarządzenia Nr 16/2016

Burmistrza Miasta Lubawka

z dnia 01 marca 2016 roku

INSTRUKCJA

ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

W URZĘDZIE MIASTA LUBAWKA

Rozdział I

Postanowienia ogólne

§ 1

Instrukcja zarządzania systemem informatycznym zwana dalej „instrukcją", jest dokumentem regulującym zasady oraz procesy zarządzania i administrowania systemami informatycznymi Urzędu Miasta Lubawka, w celu bezpiecznego ich przetwarzania.

§ 2

1. Instrukcja określa ogólne zasady i tryb postępowania Administratora Danych Osobowych oraz wszystkich użytkowników przetwarzających dane osobowe w systemie informatycznym Urzędu Miasta Lubawka.
2. Podstawa prawna:
   a) Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych – tekst jednolity Dz. U. z 2014r. poz. 1182 ze zm.
   b) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

§ 3

Określenia i skróty użyte w instrukcji oznaczają:

1. **Urząd** – Urząd Miasta Lubawka,
2. **Administrator Danych Osobowych** – Burmistrz Miasta Lubawka, zwany dalej **ADO**,
3. **Administrator Bezpieczeństwa Informacji** – pracownik urzędu lub inna osoba wyznaczona przez ADO, do nadzorowania przestrzegania zasad ochrony określonych w niniejszym dokumencie, oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych, zwana dalej **ABI**,
4. **Administrator Systemów Informatycznych,** zwany dalej **ASI** – osoba odpowiedzialna za funkcjonowanie systemu informatycznego urzędu oraz stosowanie technicznych i organizacyjnych środków ochrony i zabezpieczeń przewidzianych w systemach informatycznych,
5. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
6. **Bezpieczeństwo systemu informatycznego** – wdrożenie przez ADO lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz

ochrony danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz nieuprawnioną zmianą, utratą uszkodzeniem lub zniszczeniem,

7. **Dane osobowe** – wszelkie informacje w wersji tradycyjnej i elektronicznej dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
8. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnym wg. określonych kryteriów,
9. **Przetwarzanie danych osobowych** – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie,
10. **Osoba upoważniona lub użytkownik systemu** – osoba posiadająca upoważnienie wydane przez ADO lub uprawnioną przez niego osobę i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej, zwana dalej **użytkownikiem**. Użytkownikiem może być pracownik urzędu, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż lub praktykę w urzędzie,
11. **Przełożony użytkownika** – kierownik, osoba odpowiedzialna za przestrzeganie zasad przetwarzania i ochrony danych przez podległych mu pracowników,
12. **Osoba uprawniona** – osoba posiadająca upoważnienie wydane przez ADO do wykonywania w jego imieniu określonych czynności.

Rozdział II

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym

§ 4

1. Każdy pracownik Urzędu zobowiązany jest zapoznać się z ustawą o ochronie danych osobowych, polityką bezpieczeństwa i niniejszą instrukcją i stosować ich przepisy na swoim stanowisku pracy.
2. Przetwarzania danych osobowych może dokonywać jedynie użytkownik systemu upoważniony przez ADO i ma prawo do wykonywania tylko tych czynności, do których został upoważniony – karta nadania/cofnięcia uprawnień stanowiąca załącznik Nr 1.
3. Ewidencję uprawnień w zakresie dostępu do systemu informatycznego dokonuje ASI na podstawie otrzymanej karty nadania/cofnięcia dostępu – załącznik Nr 2.
4. Nadużycie przez użytkownika systemu postanowień niniejszej instrukcji, może stanowić podstawę do pociągnięcia go do odpowiedzialności przewidzianej właściwymi przepisami prawa.
5. Użytkownik systemu, który przetwarza dane osobowe, zobowiązany jest do zachowania tajemnicy. Tajemnica obowiązuje go również po ustaniu zatrudnienia.

6. Odebranie uprawnień użytkownikowi systemu następuje w oparciu o pismo ABI zawierające datę i przyczynę, m. In.:

   - w związku ze zmianą zakresu zadań,

   - w związku z zakończeniem stosunku pracy, zadania wynikającego z umowy cywilno-prawnej, stażu lub praktyki,

   - inną utratą uprawnień.

§ 5

Naczelną zasadą bezpieczeństwa systemu informatycznego jest ochrona informacji przed nieuprawnionym dostępem, ujawnieniem, przypadkowym lub nieautoryzowanym zniszczeniem lub modyfikacją danych. Stosowanie zasad uwierzytelniania użytkowników ma podstawowy wpływ na zachowanie poufności, rozliczalności oraz integralności danych.

§ 6

1. Dla każdego użytkownika systemu podczas przyznawania uprawnień ASI ustala identyfikator i hasło. Ustanowione hasło ASI przekazuje użytkownikowi systemu w formie pisemnej lub ustnej.

2. W systemie informatycznym stosowane jest uwierzytelnienie użytkownika przy pomocy jego identyfikatora i hasła. Stosowanie unikalnego identyfikatora realizuje zasadę rozliczalności użytkowników systemu informatycznego.

3. Hasło należy zmienić na indywidualne podczas pierwszego logowania w systemie informatycznym.

4. W celu zapewnienia wysokiego poziomu bezpieczeństwa hasło musi zawierać co najmniej 6 znaków i zawierać jednocześnie duże i małe litery oraz cyfry lub znaki specjalne.

5. Użytkownik systemu utrzymuje hasło w tajemnicy – również po upływie jego ważności. Jest odpowiedzialny za zachowanie poufności swoich haseł i powinien wprowadzać nowe hasło w taki sposób, który uniemożliwia innym osobom jego poznanie.

6. Hasło jest wpisywane i przechowywane w systemie informatycznym w postaci zaszyfrowanej.

7. Identyfikator użytkownika nie powinien być zmieniany.

8. Hasło użytkownika systemu, który utracił uprawnienia dostępu do danych osobowych unieważnia się bezzwłocznie oraz podejmuje inne niezbędne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

9. Osobą odpowiedzialną za prawidłowe funkcjonowanie mechanizmów zawartych w § 5 jest ASI.

10. Użytkownik systemu ponosi odpowiedzialność za czynności wykonane w systemie przy użyciu identyfikatora i hasła, którymi się posługuje i zobowiązany jest do utrzymania haseł dostępu w tajemnicy, a w szczególności do dołożenia wszelkich starań w celu uniemożliwienia zapoznania się z nimi osób trzecich nawet po ustaniu ich ważności.

11. Identyfikator użytkownika systemu, który utracił uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować z systemu informatycznego, w którym są one przetwarzane oraz unieważnić jego hasło.

§ 7

1. ASI prowadzi „Ewidencję użytkowników systemu osób posiadających uprawnienia do przetwarzania danych osobowych", która zawiera:

   - imię i nazwisko użytkownika,

   - zakres uprawnień,

   - nazwę identyfikatora,

   - datę zarejestrowania w systemie,

   - datę wyrejestrowania z systemu.

2. Jakakolwiek zmiana informacji wyszczególnionych w ewidencji podlega natychmiastowemu odnotowaniu.

Rozdział III

Procedury rozpoczęcia, zawieszenia, zakończenia pracy w systemie informatycznym

§ 8

1. Użytkownik systemu rozpoczynający pracę zobowiązany jest przestrzegać procedur, które mają na celu sprawdzenie zabezpieczenia pomieszczenia, w którym przetwarzane są dane osobowe, swojego stanowiska pracy oraz stanu sprzętu komputerowego.

2. Użytkownik systemu przed przystąpieniem do przetwarzania danych powinien zalogować się w systemie, posługując się swoim identyfikatorem i hasłem.

3. Użytkownik systemu w czasie pracy powinien stosować przedsięwzięcia zapewniające bezpieczeństwo przetwarzania danych osobowych w systemie:

   - ustawić ekrany monitorów w pomieszczeniach tak, aby uniemożliwić podgląd osobom nieuprawnionym,

- w przypadku przekroczenia 10 minut braku aktywności następuje automatyczna blokada systemu bądź automatyczny wygaszacz ekranu chroniony hasłem.

4. Przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane informacje lub dane poprzez zabezpieczenie komputera lub wylogowanie się z systemu.
5. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i sprawdzić, czy nie zostały pozostawione bez nadzoru nośniki informacji (płyty CD, dyski pamięci USB, itp.).
6. Użytkownik w pełnym zakresie odpowiada za powierzony sprzęt komputerowy i wykonywane czynności aż do momentu rozliczenia ze sprzętu komputerowego.

Rozdział IV

Procedury tworzenia kopii zapasowych

§ 9

1. W urzędzie stosowana jest polityka przetwarzania danych w bazach danych na dedykowanych dla systemu informatycznego serwerach.
2. Kopie zapasowe baz danych zlokalizowanych na serwerach wykonywane są w cyklach:
   - w cyklu dobowym (w godzinach nocnych) za pomocą programów archiwizujących, tworzone są pełne kopie baz danych,
   - w cyklu tygodniowym – tworzone są kopie aplikacji,
   - w cyklu podyktowanym potrzebami własnymi urzędu oraz przepisami prawa.
3. W przypadku braku technicznych możliwości sporządzenia kopii zgodnie z planem, należy je wykonać w najbliższym możliwym terminie.
4. Kopie zapasowe tworzone są na macierzy danych.
5. Kopiami zapasowymi, zgodnie z rozporządzeniem, zabezpiecza się zarówno dane jak i programy służące do ich przetwarzania.
6. Za systematyczne przygotowanie kopii bezpieczeństwa odpowiada ASI.
7. Użytkownicy systemu we własnym zakresie odpowiadają za sporządzanie kopii zapasowych i awaryjnych wytworzonych przez siebie dokumentów i danych znajdujących się na lokalnych dyskach twardych wykorzystywanych przez nich stacji roboczych. Jednocześnie maja obowiązek dopilnowania, by dane przetwarzane przy pomocy oprogramowania nie przeznaczonego do przetwarzania danych osobowych bądź też oprogramowania służącego przetwarzaniu danych osobowych wyłącznie w celu ich udostępnienia na piśmie, i zapisywane na nośnikach informatycznych nie zawierały danych osobowych.

Rozdział V

Sposób, miejsce i czas przechowywania elektronicznych nośników

(w tym kopii zapasowych).

§ 10

1. Dane w postaci elektronicznej przetwarzane w systemie zapisane na dyskietkach, dyskach, taśmach, dyskach twardych są własnością Urzędu.
2. Wymienne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych określony w Polityce Bezpieczeństwa. Po zakończeniu pracy przez użytkowników systemu, nośniki te są przechowywane w zamykanych szafach biurowych.
3. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy jest to możliwe uszkadza w sposób uniemożliwiający ich odczytanie.
4. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych pozbawia się wcześniej zapisu tych danych.
5. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do naprawy, pozbawia się wcześniej zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej
6. Kopii awaryjnych wykonywanych na nośnikach magnetycznych nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco. Przechowuje się je w miejscach zabezpieczonych przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
7. Kopie awaryjne należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu.
8. Kopie awaryjne usuwane są niezwłocznie po ustaniu ich użyteczności.

Rozdział VI

Sposób zabezpieczenia systemu informatycznego – środki ochrony

§ 11

1. W celu zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych należy zastosować środki bezpieczeństwa na poziomie wysokim.
2. Za ochronę antywirusową odpowiada ASI, który wykonuje związane z tym czynności wykorzystując moduły programu antywirusowego w aktualnej wersji – programy sprawdzające na bieżąco zasoby systemu informatycznego. Program antywirusowy powinien automatycznie sygnalizować obecność wirusów oraz niebezpiecznego oprogramowania ułatwiającego zdalny dostęp do informacji oraz posiadać mechanizmy uaktualniania bazy danych wirusów.
3. Oprogramowanie antywirusowe jest instalowane na serwerze oraz na wszystkich stanowiskach komputerowych podłączonych do systemu informatycznego.
4. Aktualizacja oprogramowania antywirusowego odbywa się automatycznie dla wszystkich zainstalowanych aplikacji nie rzadziej niż raz w tygodniu.
5. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia.
6. O każdorazowym wykryciu wirusa użytkownik zobowiązany jest niezwłocznie powiadomić ASI, który dokonuje analizy problemu i podejmuje stosowne działania naprawcze.
7. Dodatkowo należy zastosować sprzętowe urządzenia oddzielające sieć komputerową od bezpośredniego dostępu do Internetu, typu zarządzany router, stanowiące blokadę przed nieuprawnionym dostępem z zewnątrz do systemu informatycznego urzędu.
8. W sytuacji konieczności podłączenia do systemu komputerowego nośnika informacji pochodzącego z zewnętrznego źródła (np. płyty cd/dvd, pamięci usb, itp.), nośnik taki musi zostać poddany weryfikacji pod kątem infekcji szkodliwym oprogramowaniem przez ASI. Zabrania się używania do codziennej pracy urządzeń pamięci masowej nie będących na wyposażeniu urzędu i nie zatwierdzonych przez ASI.
9. Zabrania się używania i wynoszenia urządzeń i nośników informacji wykorzystywanych do pracy w urzędzie poza obszar przetwarzania danych. W przypadku zaistnienia takiej konieczności, należy uzyskać zgodę ADO/ABI. Jeśli nośnik danych umożliwiający zapis (dyskietka, pamięć usb, itp.) został podłączony do zewnętrznego urządzenia (np. komputer domowy, stacja robocza w jednostce podległej, itp.) przed jego ponownym podłączeniem do systemu informatycznego urzędu musi zostać poddany weryfikacji jak pkt. 6.

§ 12

Wymagania, które powinien spełniać system informatyczny służący do przetwarzania danych osobowych

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym – z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – system ten powinien zapewniać odnotowanie:

a) daty pierwszego wprowadzenia danych do systemu,

b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, cyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,

c) źródła danych w przypadku zbierania danych, nie od osoby, której one dotyczą,

d) informacji o odbiorcach, w rozumieniu art. 7 pkt. 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych,

e) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt. 8 ustawy.

Rozdział VII

Sposób dokonywania przeglądów i konserwacji systemu oraz zbiorów danych osobowych

§ 13

1. Okresowe oraz bieżące przeglądy i konserwacje sprzętu komputerowego, wynikające z eksploatacji, warunków zewnętrznych oraz ważności systemu dla funkcjonowania Urzędu Miasta Lubawka wykonuje ASI. Powinny być one wykonywane w terminach określonych przez producenta sprzętu.

2. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do naprawy w firmach zewnętrznych, pozbawia się przed naprawą zapisu danych osobowych, albo naprawia je pod nadzorem ASI.

3. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do likwidacji należy pozbawić zapisu, a w przypadku, gdy jest to niemożliwe, uszkodzić mechanicznie w sposób uniemożliwiający ich odczytanie.

4. Przegląd programów i narzędzi programowych – konserwacja baz danych przeprowadzana jest zgodnie z zaleceniami twórców poszczególnych programów.

5. ASI zobowiązany jest uaktywnić mechanizm zaliczania nieudanych prób zameldowania do systemu oraz ustawić blokadę konta użytkownika po wykryciu trzech nieudanych prób we wszystkich systemach posiadających taką funkcję.

Załącznik Nr 1

do „Instrukcji Zarządzania Systemem Informatycznym

w Urzędzie Miasta Lubawka"

Karta nadania/cofnięcia uprawnień

□ Nowy użytkownik	□ Nadanie uprawnień w systemie informatycznym /modyfikacja	□ Odebranie uprawnień w systemie informatycznym
Imię i nazwisko użytkownika	Stanowisko	
Opis zakresu uprawnień użytkownika w systemie informatycznym i uzasadnienie		
Data wystawienia	Podpis bezpośredniego przełożonego użytkownika systemu:	
Nadaję identyfikator:	Podpis Kierownika	

§ 14

Dane osobowe zapisane na urządzeniach i nośnikach informacji, o których mowa w art. 27 ust. 1 ustawy, przekazywane poza obszar przetwarzania danych osobowych, w celu zapewnienia ich poufności i integralności, powinny wcześniej zostać zakodowane stosownym programem przy użyciu ca najmniej 7 literowego hasła, które musi zawierać duże i małe litery oraz cyfry lub znaki specjalne.

Rozdział VIII

Postanowienia końcowe

§ 15

1. Użytkownik systemu informatycznego nie ma prawa dokonywania samodzielnych instalacji, deinstalacji jakiegokolwiek oprogramowania, ani wprowadzania zmian w konfiguracji oprogramowania, ani wprowadzania zmian w konfiguracji oprogramowania wykraczających poza jego normalne użytkowanie.
2. Czynności, o których mowa w § 15 pkt. 1 wykonuje ASI.
3. ABI prowadzi „Rejestr zbiorów danych osobowych przetwarzanych w systemach informatycznych".
4. ASI przeprowadza szkolenia dla nowozatrudnionych pracowników oraz w przypadku istotnych zmian w systemach informatycznych, w których przetwarzane są dane osobowe z zakresu stosowania Instrukcji Zarządzania Systemem Informatycznym.
5. ABI dokonuje okresowego sprawdzenia sprawności funkcjonowania zabezpieczeń systemów, w których przetwarzane są dane osobowe.

§ 16

W sprawach nieuregulowanych niniejszą Instrukcją zastosowanie znajdują przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tj. Dz. U. z 2014r. poz. 1182 ze zm.), Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024).

Załącznik Nr 2

do „Instrukcji Zarządzania Systemem Informatycznym

w Urzędzie Miasta Lubawka"

EWIDENCJA UPRAWNIEŃ W ZAKRESIE DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

W URZEDZIE MIASTA LUBAWKA

L.p.	Nazwisko i imię użytkownika	Zakres uprawnień	Identyfikator	Data rejestracji w systemie	Data wyrejestrowania z systemu	Podpis ASI

Sporządziła:

Magdalena Trybuchowska-Łabencka

Kierownik Ref. OELiUSC